Statement by the Submitter

I, Bruce Schneier, do hereby declare that to the best of my knowledge the practice of the algorithm, reference implementation, and mathematically optimized implementations, I have submitted, known as Twofish may be covered by the following U.S. and/or foreign patents: none.

I do hereby declare that I am aware of no patent applications which may cover the practice of my submitted algorithm, reference implementation or mathematically optimized implementations.

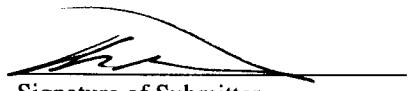
I hereby declare that we intend to file for patent applications that may cover the practice of my submitted algorithm, referenced implementation or optimized implementations. I hereby agree to inform NIST of their application numbers as soon as possible after they are filed by submitting a completed 2.D.2 statement.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Advanced Encryption Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for inclusion in the Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES). I further understand that I will not receive financial compensation from the government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the AES or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for inclusion in the AES, I hereby agree not to place any restrictions on the use of the algorithm intending it to be available on a worldwide, non-exclusive, royalty-free basis.

I do hereby agree to provide the statements required by sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover practice of my algorithm, reference implementation or mathematically optimized implementations and the right to use such implementations for the purposes of the AES evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for inclusion in the FIPS (including those not selected for second round of public evaluation), I understand that all rights, including use rights of the reference and mathematically optimized implementations, revert back to the submitter (and other owner[s] as appropriate). Additionally, should the U.S. Government not select my algorithm for inclusion in the AES after a period of four years from the close of the submission date for candidate algorithms, all rights revert to the submitter (and other owner[s] as appropriate).

Agreed to and Accepted



Signature of Submitter

Printed Name: Bruce Schneier

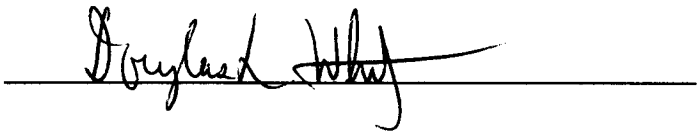
Title: President, Counterpane Systems

Dated: 15 June 1998

Place: Minneapolis, MN

Statement by the Reference/Mathematically Optimized Implementations' Owner(s)

Hi/fn is the owner of the submitted reference implementation and mathematically optimized implementations and hereby grants the Government and any interested party the right to use such implementations for the purposes of the AES evaluation process notwithstanding that the implementations may be copyrighted.

Signed: 

Name: Douglas L. Whiting

Title: Chief Technology Officer, Hi/fn

Dated: June 1, 1998

Place: San Diego, California

Permission and Author's Copyright Release

I, Bruce Schneier, do hereby grant the National Institute of Standards and Technology (NIST) the nonexclusive right to reproduce or to have reproduced, prepare or have prepared in derivative form, and distribute or have distributed copies of all materials submitted to NIST in my Advanced Encryption Standard candidate nomination.

I also represent that the exercise of these rights by NIST will not infringe or otherwise violate any rights or another person or organization.

Agreed to and Accepted

Signature of Submitter

Printed Name: Bruce Schneier

Title: President, Counterpane Systems

Dated: 15 June 1998

Place: Minneapolis, MN